

# United States District Court

for the  
Western District of New York



## In the Matter of the Search of

*(Briefly describe the property to be searched or identify the person by name and address.)*

Two Portable Document Files ("the PDFs"), which contain text messages sent to, and received by, the account +17278886881. Account +17278886881 is owned, maintained, controlled, or operated by Secret Phone, which is owned by BP Mobile LLC, 6799 Collins Ave Office 1602, Miami Beach, FL 33141. BP Mobile provided the PDFs, by email, to FBI Buffalo on January 27, 2020. The PDFs are currently in the electronic possession of FBI Buffalo.

Case No. 20-mj- 5036

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: **See Attachment A, which is attached hereto and incorporated by reference herein,**

Located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

**Evidence, contraband, fruits and instrumentalities pertaining to violations of 18 U.S.C. § 1030, 18 U.S.C. § 1028A, and 18 U.S.C. § 2252A(a), as more fully set forth in Attachment B, which is attached hereto and incorporated by reference herein.**

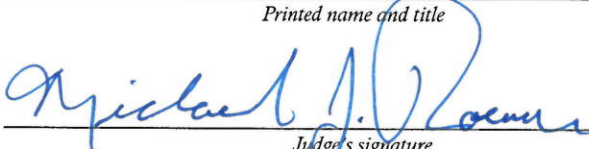
The basis for search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of 18 U.S.C. § 1030, 18 U.S.C. § 1028A, and 18 U.S.C. § 2252A(a). The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature  
COREY LYONS  
SPECIAL AGENT  
FEDERAL BUREAU OF INVESTIGATION  
Printed name and title

  
Judge's signature  
HONORABLE MICHAEL J. ROEMER  
UNITED STATES MAGISTRATE JUDGE  
Printed name and Title

Date: January 30, 2020

City and state: Buffalo, New York

**ATTACHMENT A**

This warrant authorizes the search of two Portable Document Files (“the PDFs”), which contain text messages sent to, and received by, the account +17278886881. Account +17278886881 is owned, maintained, controlled, or operated by Secret Phone, which is owned by BP Mobile LLC, 6799 Collins Ave Office 1602, Miami Beach, FL 33141. BP Mobile provided the PDFs, by email, to FBI Buffalo on January 27, 2020. The PDFs are currently in the electronic possession of FBI Buffalo.

**ATTACHMENT B**

All records or information, in whatever form, including the contents of any and all wire and electronic communications, attachments, stored files, print outs, and header information that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1030 (unauthorized access to computer systems); 18 U.S.C. § 1028A (aggravated identity theft); and/or 18 U.S.C. § 2252A(a) (receipt, distribution, and possession of child pornography) including information pertaining to:

- a. The unauthorized access of Snapchat accounts. Such evidence includes records of IP logins that match those of Snapchat accounts after their original user lost access, as well as records and communications concerning password resets, user names, and answers to security questions
- b. Records and communications concerning the impersonation of others; the targeting of victims for such schemes; and material obtained from such schemes, including personal information, photographs, and videos;
- c. All visual depictions, including still images, videos, films or other recordings of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or engaged in sexually suggestive conduct (such as exposing and/or touching their breasts or genitalia);
- d. Communications revealing the request for, and the obtainment of, victims' Snapchat login credentials;
- e. Communications or records concerning the age of the individuals shown in any photograph or video accessed from any Snapchat account.

**AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT**

STATE OF NEW YORK     )  
COUNTY OF ERIE         )     SS:  
CITY OF BUFFALO         )

I, Corey Lyons, being duly sworn, depose and state the following:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since May 12, 2019. I am currently assigned to the Cyber Task Force, Buffalo Division. As part of the Cyber Task Force, I work on investigations relating to criminal and national security cyber intrusions. I received training on cyber matters during my time in Quantico, VA and have received private sector cyber training. I have worked or assisted with matters involving unauthorized access to computer systems, internet fraud, and business email compromises. My work in the FBI, as well as training I have received, has familiarized me with identifying and handling evidence found in digital media, network analysis, and digital forensics. I am familiar with fundamental operations of the internet, hardware, software, and the communication protocols across each. Experience with similar investigations and working with other FBI Special Agents and computer forensic professionals has expanded my knowledge of internet communications. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, mobile phones and tablets, and electronically stored information, in conjunction with criminal investigations. I have also conferred with other FBI Special Agents who have expertise and experience in cyber investigations and digital evidence.

2. I make this affidavit in support of an application for a search warrant authorizing the search of two Portable Document Format files ("the PDFs") containing text messages sent to, and received by, the phone number +17278886881.<sup>1</sup> These PDFs were sent to FBI Buffalo via email on January 27, 2020 by Secret Phone, which is owned by BP Mobile LLC, 6799 Collins Ave Office 1602, Miami Beach, FL 33141. The PDFs are currently in FBI Buffalo's electronic possession. This affidavit is made in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 to allow the government to review the PDFs, which include the content of text messages.

3. I respectfully submit that probable cause exists to believe that evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. § 1030 (unauthorized access to computer systems), 18 U.S.C. § 1028A (aggravated identity theft), and 18 U.S.C. § 2252A(a) (receipt, distribution, and possession of child pornography) will be found in the PDFs.

4. I am familiar with the facts contained in this affidavit based upon my personal involvement in this investigation, information provided by other law enforcement agents, particularly agents from the Buffalo Field Office of the FBI, and private companies. Because this affidavit is submitted for the limited purpose of obtaining this search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause.

#### **BACKGROUND REGARDING SECRET PHONE**

---

<sup>1</sup> A PDF is an electronic file format that, among other things, can display text or graphics in a manner similar to a traditional printed document.

5. Based on my training and experience, I have learned the following about Secret Phone, also known as Second Phone Number:

- a. Secret Phone is a mobile application made by BP Mobile and available through the iPhone App Store and Google Play. The application allows users to acquire a private phone number for calls and texts.
- b. Secret Phone allows users to pick a phone number and purchase credits that allow them to make calls and texts from that number. Users can choose a phone number from a list of available numbers in 25 different countries. Users are able to view their text message history and forward calls to voice mail.

#### OVERVIEW OF INVESTIGATION

6. On or about December 5, 2019, FBI Buffalo received information regarding a potential compromise and the victimization of a State University of New York (SUNY) Geneseo student NC's Snapchat account, **blinkinglights1**. According to NC, while at SUNY Geneseo, in Geneseo, New York, he/she received a message from a Snapchat user (UNSUB) he/she believed to be DF. NC knew of DF through a mutual acquaintance. The UNSUB asked NC for his/her Snapchat login credentials under the ruse that they would use NC's account to check to see if DF had been "blocked" by another user.

7. NC provided his/her Snapchat login credentials to the UNSUB and soon after received a text message from an UNSUB using the phone number +1(626)-515-8283. The UNSUB was purporting to be Snapchat Security. The text message stated that NC's Snapchat account had been locked and he/she needed to provide a pin number to unlock it. The text

message also advised that the pin requested is the same pin used for NC's "My eyes only" folder in his/her Snapchat account. NC provided the pin number to the UNSUB. Shortly thereafter, NC received an email from the true Snapchat, notifying NC of a new device login to his/her account. The login was from an IPHONE X using the internet protocol address 176.113.72.166 at 17:38:56 EST on 3 December 2019. Snapchat also notified NC that the email address associated with his/her **blinkinglights1** account was changed from [natalie.m.claus@gmail.com](mailto:natalie.m.claus@gmail.com) to [garyjenny321@outlook.com](mailto:garyjenny321@outlook.com). After this occurred, NC was no longer able to access his/her account.

8. Once he/she received access to NC's account, the UNSUB sent an explicit photo of NC to all of the female Snapchat users on NC's friend list. The photo was captioned, "Flash me back if we are besties". Four of NC's friends responded back to the message by sending explicit pictures of themselves, one of whom was SS. SS stated that he/she received the message from NC's account. Once SS replied with his/her picture, he/she noticed that NC's account saved the photo, which he/she noted was unusual for NC to do. On 4 December 2019, SS received a text message from NC saying that his/her Snapchat account was hacked and apologized if anyone received suspicious messages from him/her. SS then filed a police report fearing that the UNSUB had the explicit photo he/she sent to NC's account.

9. During an interview of NC, he/she advised that multiple students from his/her hometown had their Snapchat accounts hacked in a similar way. Most, if not all, of the

victims attended Bethlehem High School, located in Delmar, New York, and had some connection to DF.

10. One of those victims, BB, filed a police report on 7 December 2019 because his/her account was hacked. According to BB, his/her Snapchat account, **brogan.bennett**, received messages from IM's Snapchat account requesting BB's login credentials for his/her Snapchat account. The individual operating IM's account claimed that he/she deleted his/her Snapchat account and wanted to login from BB's account to confirm his/her account was deleted. BB then provided who he/she believed was IM with his/her login credentials. A short time later, BB received a text message from the phone number **+17278886881**. **+17278886881** claimed to be Snapchat Security and told BB that his account was locked due to suspicious activity. **+17278886881** then requested his PIN number to unlock the account. **+17278886881** provided a hint for the PIN saying it was the same as BB's "My Eyes Only" folder PIN. After BB provided his/her login credentials and PIN, BB was locked out of his/her account.

11. The UNSUB who obtained unauthorized access to BB's account then started sending nude pictures to several of BB's friends on Snapchat. The nude photos were from AF's saved photos on his/her Snapchat account, **afresina1223**. BB stated that AF's Snapchat account was hacked a few days prior to 7 December 2019. BB claimed that the UNSUB took photos from AF's account and uploaded them to BB's account after BB lost access to the account. This allowed the UNSUB to send the photos of AF to everyone on BB's friends list.

12. According to AF, he/she was asked for his/her login credentials by an individual she thought was DF. This individual claimed that they wanted to get into AF's account to see if they had been blocked by another user. Once AF provided his/her login credentials, he/she was locked out of her account.

13. On 12 December 2019, another individual, MM, filed a police report regarding similar activity. According to MM, on 12 December 2019 he/she received a Snapchat message from the username **seabass4life**, which he/she believed to be used by SC. The message included a video and a request for him/her to watch it. When MM opened the video he/she realized that it was of him/her having sex when he/she was 15 years old. MM was unaware that SC had his/her account hacked previously. MM stated that several other Bethlehem graduates recently had their Snapchat accounts hacked.

#### **BACKGROUND REGARDING THE ATTRIBUTION OF +17278886881**

14. Open source searches for **+17278886881** showed that the number was owned by Onvoy LLC. On or about December 23, 2019 a Grand Jury Subpoena was served to Onvoy LLC for subscriber information associated with the **+17278886881** phone number. In response to the subpoena, Onvoy LLC indicated that the number was sold to Twilio. On January 10, 2020, a Grand Jury Subpoena was issued to Twilio for information associated with the **+17278886881** phone number. In response to the subpoena, Twilio indicated that it had sold the number to BP Mobile. On January 23, 2020 a Grand Jury Subpoena was issued to BP Mobile for information associated with the **+17278886881** phone number. BP Mobile provided subscriber information, as well as IP login information and call log information.

15. FBI Buffalo responded to BP Mobile by asking for timestamps associated with the IP logins; whether BP Mobile maintains text message transactional data (i.e., “to/from” information); and, if so, whether BP Mobile would require additional legal process to disclose such information. FBI Buffalo also asked if BP Mobile maintained records of the content of text messages so that FBI Buffalo could, if appropriate, request the text messages via a Search Warrant. On January 23, 2020, BP Mobile indicated that “[i]f any of the data [the FBI] mentioned is recorded on [BP Mobile’s] side we will deliver it without additional subpoena or search warrant.” On January 27, 2020, BP Mobile voluntarily provided FBI Buffalo with the PDFs, which include the content of text messages sent to and received by +17278886881, as well as IP login timestamps and the text message transactional data. Although FBI Buffalo may already have all necessary authority to review the PDFs (because BP Mobile voluntarily disclosed them to FBI Buffalo), I seek this additional warrant out of an abundance of caution to be certain that FBI Buffalo’s review of the PDFs will comply with the Fourth Amendment. In my training and experience, I know that the PDFs are designed, and have been electronically stored, in a manner in which their contents are in the same state as they were when the PDFs were first sent to FBI Buffalo.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

16. I anticipate executing this warrant by opening and reviewing the PDF files provided to FBI Buffalo by BP Mobile on January 27, 2020 and reviewing those files to locate the items described in Attachment B.

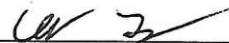
### CONCLUSION

17. Based on the foregoing, I believe there is probable cause to believe that violations of 18 U.S.C. § 1030 (unauthorized access to computer systems), 18 U.S.C. § 1028A (aggravated identity theft), and 18 U.S.C. § 2252A(a) (receipt, distribution, and possession of child pornography) have occurred, and that evidence, contraband, fruits, and instrumentalities of such violations, as more fully described in Attachment B, will be in the PDFs described in Attachment A.

18. Venue is proper in the Western District of New York because this warrant application seeks to search and seize property—i.e., the PDFs—that is currently in the possession of FBI Buffalo, within the Western District of New York.

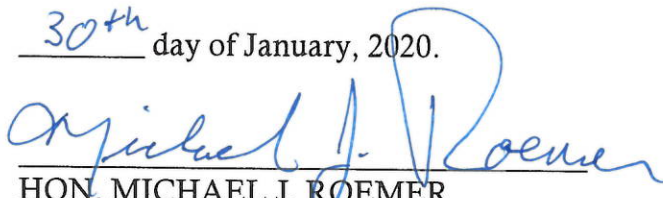
**REQUEST FOR SEALING**

19. Because this investigation is continuing, disclosure of the search warrant, this affidavit, and/or this application and the attachments thereto could jeopardize the progress of the investigation. Public disclosure of the search warrant at this time could jeopardize the investigation by giving the target(s) an opportunity to destroy evidence, change patterns of behavior, notify confederates, or flee from prosecution. Accordingly, I request that the Court issue an order that the search warrant, this affidavit in support of application for search warrant, the application for search warrant, and all attachments thereto be filed under seal until further order of this Court.

  
\_\_\_\_\_  
Corey Lyons  
Special Agent  
Federal Bureau of Investigation

Sworn and subscribed to before me this

30<sup>th</sup> day of January, 2020.

  
\_\_\_\_\_  
HON. MICHAEL J. ROEMER  
United States Magistrate Judge